On the Rank of the Elliptic Curve $y^2 = x(x-p)(x-2)$

Jeffrey Hatley*

September 9, 2009

Abstract

An elliptic curve E defined over $\mathbb{Q}$ is an algebraic variety which forms a finitely generated abelian group, and the structure theorem then implies that $E \cong \mathbb{Z}^r \oplus \mathbb{Z}_{\text{tors}}$ for some $r \geq 0$; this value r is called the rank of E. It is a classical problem in the study of elliptic curves to classify curves by their rank. In this paper, the author uses the method of $2-$descent to calculate the rank of two families of elliptic curves.

1 Introduction

An elliptic curve E defined over $\mathbb{Q}$ is the set of solutions $(x, y) \in \mathbb{Q}^2$ to an equation of the form

$$y^2 = x^3 + ax^2 + bx + c, \text{ with } a, b, c \in \mathbb{Q}$$

along with an additional point at infinity, $\mathcal{O}$. A classical theorem from Mordell shows that such an ellipic curve forms a finitely generated abelian group; the structure theorem then implies that

$$E \cong \mathbb{Z}^r \oplus \mathbb{Z}_{\text{tors}}, \ r \geq 0.$$

This nonnegative integer r is called the *rank* of the elliptic curve. It is a classical problem to classify ellipic curves, and the rank of a curve provides a useful way to distinguish it from other curves, as well as to gain some insight into its algebraic structure. However, calculating the rank of a given ellipic curve can be quite difficult in general. One method of doing so is the method of 2-descent. The machinery behind 2-descent is quite high-powered, but the idea is rather simple.

The main idea behind 2-descent is a local-to-global method. One indirectly studies an elliptic curve E by examining whether certain related equations, called *homogeneous spaces*, have rational points over every local field $\mathbb{Q}_p$ for

*Department of Mathematics and Statistics, University of Massachusetts - Amherst

$p = \infty$ or p a rational prime. This information is then pieced together to yield information about E.

This paper uses two variations on the method of two-descent to gain results on the ranks of two different families of ellipic curves. While studying computer computations of the ranks of elliptic curves of the form

$$E_p : y^2 = x(x-p)(x-2),$$

Jason Beers made the following conjecture.

Conjecture. *Let E_p be the elliptic curve defined by $E_p : y^2 = x(x-p)(x-2)$ where p and $p-2$ are twin primes. Then*

$$\operatorname{rank}(E_p) = \begin{cases} 0 & \text{if } p \equiv 7 \pmod 8, \\ 1 & \text{if } p \equiv 3, 5 \pmod 8, \\ 2 & \text{if } p \equiv 1 \pmod 8. \end{cases}$$

Curves similar to this form were considered in Silverman [1], and similar results for the curve $E : y^2 = x(x-(p-2))(x-p)$ were recently made available on arXiv.

In this paper, we prove the first case and part of the second; more specifically, we prove

Theorem 1. *Let p and $p-2$ be twin primes, and let E_p be the elliptic curve defined by $E_p : y^2 = x(x-p)(x-2)$.*

(a) *If $p \equiv 7$ (mod 8), then rank(E_p) $= 0$. In particular, we have*

$$E_p(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

(b) *If $p \equiv 5$ (mod 8), then rank(E_p) ≤ 1. In particular, we have*

$$E_p(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

or

$$E_p(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Before going through each proof, we state the method of two-descent to be used as presented in Silverman [1].

2 Proof of Theorem 1(a)

In this section we prove the following theorem:

Theorem 1(a). *Let p and $p-2$ be prime numbers in $\mathbb{Z}$ with $p \equiv 7$ (mod 8). Then the elliptic curve $E(\mathbb{Q})$ given by*

$$E : y^2 = x(x-p)(x-2)$$

has rank 0*. In particular,*

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

To prove this theorem, we use the method of 2-descent presented as Proposition 1.4 of Chapter X in Silverman [1], which we now state.

Theorem 2. (Complete 2-Descent, Version 1). *Let $E/\mathbb{Q}$ be an elliptic curve given by an equation*

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \text{ with } e_1, e_2, e_3 \in \mathbb{Q}.$$

Let S be a set of places of $\mathbb{Q}$ including $2, \infty$, and all places dividing the discriminant of E. Further, let

$$\mathbb{Q}(S, 2) = \{b \in \mathbb{Q}^*/\mathbb{Q}^{*2} : \mathrm{ord}_\nu(b) \equiv 0 (\text{mod } 2) \text{ for all } \nu \notin S\}.$$

There is an injective homomorphism

$$E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$$

defined by

$$P = (x, y) \to \begin{cases} (x - e_1, x - e_2) & \text{if } x \neq e_q, e_2 \\ ((e_1 - e_3)/(e_1 - e_2), e_1 - e_2) & \text{if } x = e_1 \\ (e_2 - e_1, (e_2 - e_3)/(e_2 - e_1)) & \text{if } x = e_2 \\ (1, 1) & \text{if } x = \infty \text{ (i.e. if } P = \mathcal{O}). \end{cases}$$

Let $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ be a pair which is not the image of one of the three points $\mathcal{O}, (e_1, 0), (e_2, 0)$. Then (b_1, b_2) is the image of a point $P = (x, y) \in E(\mathbb{Q})/2E(\mathbb{Q})$ if and only if the equations

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1$$

have a solution $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}^*$; if such a solution exists, then one can take

$$P = (x, y) = (b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3).$$

Thus, Theorem 2 allows one to calculate $E(\mathbb{Q})/2E(\mathbb{Q})$ for ellipic curves defined by a sufficiently nice equation. If $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \mathbb{Z}_{\text{tors}}$, then all of the odd-torsion (i.e. factors of $E(\mathbb{Q})$ of the form $\mathbb{Z}/m\mathbb{Z}$ where m is odd) is killed in $E(\mathbb{Q})/2E(\mathbb{Q})$. Furthermore, if p is a prime of good reduction for E and gcd(p, m)=1, then $E(\mathbb{Q})[m]$ injects into $\tilde{E}(\mathbb{F}_p)$, the $\mathbb{F}_p$ rational points on the reduction of E modulo p, so it is easy to calculate E_{tors}. These facts together

with Theorem 2 allow one to calculate the rank of certain elliptic curves. We now prove Theorem 1(a).

Proof of Theorem 1(a).
Our curve is

$$E : y^2 = x(x-p)(x-2) = x^3 - (p+2)x^2 + 2px$$

which has discriminant $\Delta = 2^2 p^2 (p-2)^2$, so our set S is

$$S = \{2, p, p-2\}$$

and our set $\mathbb{Q}(S,2)$ is

$$\mathbb{Q}(S,2) = \{\pm 1, \pm 2, \pm p, \pm(p-2), \pm 2p, \pm 2(p-2), \pm p(p-2), \pm 2p(p-2)\}.$$

The two-torsion points of $E(\mathbb{Q})$ are those points $(x,y) \in E(\mathbb{Q})$ with $y = 0$, hence the two-torsion of our curve is

$$E(\mathbb{Q})[2] = \{\mathcal{O}, (0,0), (2,0), (p,0)\}.$$

Now, since $p \geq 7$, we have $3 \nmid \Delta$, and so we see that E_{tors} injects into $E(\mathbb{F}_3)$. By hypothesis $p = 7 + 8k$ for some non-negative integer k. In fact, $k \equiv 0 \pmod 3$, since if $k \equiv 1 \pmod 3$ then $p \equiv 0 \pmod 3$ and so is not prime; likewise, if $k \equiv 2 \pmod 3$, then $p - 2 \equiv 0 \pmod 3$, so $p-2$ is not prime. Hence we have $k \equiv 0 \pmod 3$, and

$$E(\mathbb{F}_3) = \{\mathcal{O}, (0,0), (1,0), (2,0)\}$$

where the fact that $(1,0) \in E$ follows from our congruence argument on k. Any odd $m-$torsion must be an $m-$group, and since $E[2] \subset E_{\text{tors}}$ and both $E[2]$ and $E(\mathbb{F}_3)$ have cardinality 4, we see that $E_{\text{tors}} = E[2]$.

Now we consider the map

$$\phi : E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$$

given in Theorem 2 with $e_1 = 0$, $e_2 = 2$, and $e_3 = p$. There are 256 pairs $(b_1, b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$, and for each pair we must check to see whether it comes from an element of $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$. Using Theorem 2, we can compute the image $\phi(E[2])$ in $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$:

$$\mathcal{O} \to (1,1) \quad (0,0) \to (2p, -2) \quad (2,0) \to (2, -2(p-2)) \quad (p,0) \to (p, p-2).$$

For the remaining pairs (b_1, b_2) we must determine whether the equations

$$b_1 z_1^2 - b_2 z_2^2 = 2 \tag{1}$$

and

$$b_1 z_1^2 - b_1 b_2 z_3^2 = p \tag{2}$$

have a simultaneous solution $(z_1, z_2, z_3) \in \mathbb{Q}^3$. This is facilitated by a few facts. First, recall that $\mathbb{Q} \subset \mathbb{Q}_q$ (the q-adic completion of $\mathbb{Q}$) for each prime q, so if an equation has no solutions over $\mathbb{Q}_q$ then it has no solutions over $\mathbb{Q}$, and the pair (b_1, b_2) in that case is not in $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$. Second, the map ϕ is a homomorphism. Thus, if (b_1, b_2) and (b_1', b_2') are both in the image of ϕ, then so is $(b_1 b_1', b_2 b_2')$; if (b_1, b_2) is in the image and (b_1', b_2') is not, then $(b_1 b_1', b_2 b_2')$ is not. If the equations corresponding to a pair (b_1, b_2) have no solutions over some $\mathbb{Q}_p$, we say that (b_1, b_2) is $\mathbb{Q}_p$-*non-trivial*.

We follow Silverman's lead and list our results in a table whose entries list either the point $(x, y) \in E(\mathbb{Q})$ that gets mapped to the pair (b_1, b_2) or the field over which the equations (1) and (2) have no solution. If (z_1, z_2, z_3) is a solution to equations (1) and (2), then the pre-image of (b_1, b_2) is $(b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3)$. Each table entry also has a superscript number (n) which refers to a note explaining the entry. We do exclude half of the points from the table, however: it is easy to see that if $b_1 < 0$ and $b_2 > 0$ then equation (1) has no solutions in $\mathbb{R}$, and if $b_1 < 0$ and $b_2 < 0$ then equation (2) has no solution in $\mathbb{R}$. Hence, we exclude the portion of the table with $b_1 < 0$.

$b_1 \backslash b_2$	1	2	p	$p-2$	$2p$	$2(p-2)$	$p(p-2)$	$2p(p-2)$
1	$\mathcal{O}$	$\mathbb{Q}_2^{(3)}$	$\mathbb{Q}_p^{(5)}$	$\mathbb{Q}_{p-2}^{(7)}$	$\mathbb{Q}_2^{(3)}$		$\mathbb{Q}_p^{(5)}$	$\mathbb{Q}_2^{(3)}$
2	$\mathbb{Q}_2^{(4)}$	$\mathbb{Q}_{p-2}^{(12)}$	$\mathbb{Q}_2^{(4)}$		$\mathbb{Q}_p^{(16)}$	$\mathbb{Q}_{p-2}^{(16)}$	$\mathbb{Q}_2^{(4)}$	$\mathbb{Q}_p^{(14)}$
p	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(3)}$	$\mathbb{Q}_p^{(12)}$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(3)}$		$\mathbb{Q}_p^{(10)}$	$\mathbb{Q}_2^{(3)}$
$p-2$	$\mathbb{Q}_p^{(6)}$		$(p,0)$	$\mathbb{Q}_p^{(6)}$			$\mathbb{Q}_{p-2}^{(3)}$	
$2p$	$\mathbb{Q}_2^{(4)}$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(4)}$		$\mathbb{Q}_p^{(10)}$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(4)}$	$\mathbb{Q}_p^{(10)}$
$2(p-2)$		$\mathbb{Q}_p^{(14)}$			$\mathbb{Q}_{p-2}^{(12)}$	$\mathbb{Q}_p^{(14)}$		$\mathbb{Q}_{p-2}^{(16)}$
$p(p-2)$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(3)}$	$\mathbb{Q}_p^{(10)}$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(3)}$		$\mathbb{Q}_2^{(4)}$	$\mathbb{Q}_2^{(3)}$
$2p(p-2)$	$\mathbb{Q}_2^{(4)}$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(4)}$		$\mathbb{Q}_p^{(10)}$	$\mathbb{Q}_p^{(9)}$		$\mathbb{Q}_p^{(10)}$
-1	$\mathbb{Q}_p^{(14)}$	$\mathbb{Q}_2^{(3)}$	$\mathbb{Q}_{p-2}^{(12)}$	$\mathbb{Q}_p^{(14)}$	$\mathbb{Q}_2^{(3)}$		$\mathbb{Q}_{p-2}^{(15)}$	$\mathbb{Q}_2^{(3)}$
-2	$\mathbb{Q}_2^{(4)}$	$\mathbb{Q}_p^{(6)}$	$\mathbb{Q}_2^{(4)}$		$(0,0)$	$\mathbb{Q}_p^{(6)}$	$\mathbb{Q}_2^{(4)}$	$\mathbb{Q}_{p-2}^{(8)}$
$-p$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(3)}$	$\mathbb{Q}_p^{(10)}$	$\mathbb{Q}_p^{(11)}$	$\mathbb{Q}_2^{(3)}$		$\mathbb{Q}_p^{(10)}$	$\mathbb{Q}_2^{(3)}$
$-(p-2)$	$\mathbb{Q}_{p-2}^{(11)}$		$\mathbb{Q}_p^{(13)}$	$\mathbb{Q}_{p-2}^{(16)}$			$\mathbb{Q}_p^{(13)}$	
$-2p$	$\mathbb{Q}_2^{(4)}$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(4)}$		$\mathbb{Q}_p^{(10)}$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(4)}$	$\mathbb{Q}_p^{(10)}$
$-2(p-2)$		$(2,0)$			$\mathbb{Q}_p^{(6)}$	$\mathbb{Q}_{p-2}^{(8)}$		$\mathbb{Q}_p^{(6)}$
$-p(p-2)$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(3)}$	$\mathbb{Q}_p^{(10)}$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(3)}$		$\mathbb{Q}_p^{(10)}$	$\mathbb{Q}_2^{(3)}$
$-2p(p-2)$	$\mathbb{Q}_2^{(4)}$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(4)}$		$\mathbb{Q}_p^{(10)}$	$\mathbb{Q}_p^{(9)}$	$\mathbb{Q}_2^{(4)}$	$\mathbb{Q}_p^{(10)}$

Notes For Table

1. If $b_1 < 0$ and $b_2 > 0$, equation (1) has no solutions in $\mathbb{R}$.

2. If $b_1 < 0$ and $b_2 < 0$, equation (2) has no sution in $\mathbb{R}$.

3. Suppose there exists a solution (z_1, z_2, z_3). We have $b_1 \equiv 0 \pmod 2$ and $b_2 \not\equiv 0 \pmod 2$. Then comparing $2-$adic valuations of the left-hand and right-hand sides of equation (1) easily implies $z_1, z_2 \in \mathbb{Z}_2$. But then $b_1 z_1^2 - b_1 b_2 z_3^2 \equiv 0 \pmod 2$, so equation (2) implies $p \equiv 0 \pmod 2$. Since p is odd, this is a contradiction, so equations (1) and (2) have no solutions over $\mathbb{Q}_2$

4. Adding the $\mathbb{Q}_2$-non-trivial pairs from (3) to the (pairs corresponding to the) points in $E[2]$ yields these $\mathbb{Q}_2$-non-trivial pairs.

5. If $(b_1, b_2) = (p, 1)$ or $(p(p-2), 1)$, then valuation arguments again show that any solution (z_1, z_2, z_3) has $z_1, z_2 \in \mathbb{Z}_p$, hence equation (1) becomes

$$z_2^2 \equiv -2 \pmod p$$

which has no solutions since $p \equiv 7 \pmod 8$.

6. Adding the pairs from (5) to the points in $E[2]$ yields these $\mathbb{Q}_p$-non-trivial points.

7. If $(b_1, b_2) = (p-2, 1)$, then again $z_1, z_2 \in \mathbb{Z}_{p-2}$, so equation (1) implies

$$z_2^2 \equiv -2 \pmod{(p-2)},$$

which has no solutions since $p - 2 \equiv 5 \pmod 8$.

8. Adding the pairs from (7) yields these $\mathbb{Q}_{p-2}$-non-trivial points.

9. Suppose $b_2 \equiv 0 \pmod p$ and $b_1 \not\equiv 0 \pmod p$, and suppose there exists a solution (z_1, z_2, z_3). Let

$$k = \nu_p(z_1), \quad j = \nu_p(z_2, \quad l = \nu_p(z_3.$$

Then equation (2) implies that

$$\begin{aligned} 1 &= \nu_p(b_1 z_1^2 - b_1 b_2 z_3^2) \\ &= min\{2k, 1 + 2l\} \end{aligned}$$

which implies $l = 0$ and $k > 0$. But equation (1) implies

$$\begin{aligned} 0 &= \nu_p(b_1 z_1^2 - b_2 z_2^2) \\ &= min\{2k, 1 + 2j\} \end{aligned}$$

which implies $k = 0$, which is a contradiction. Hence equations (1) and (2) have no solutions over $\mathbb{Q}_p$ in his case.

10. Adding pairs from (9) to the points in $E[2]$ yields these $\mathbb{Q}_p$-non-trivial pairs.

11. If $(b_1, b_2) = (1, -(p-2))$, then once again equation (1) implies $z_1, z_2 \in \mathbb{Z}_{p-2}$. Subtracting p from both sides of equation (1) yields

$$z_1^2 + (p-2)z_2^2 - p = 2 - p,$$

so looking modulo $(p-2)$ we have

$$z_1^2 \equiv p \equiv 2 \pmod{(p-2)}).$$

But $p - 2 \equiv 5 \pmod 8$, so no such z_1 exists, hence equation (1) has no solutions over $\mathbb{Q}_{p-2}$.

12. Adding pairs from (11) to the points in $E[2]$ yields these $\mathbb{Q}_{p-2}$-non-trivial pairs.

13. If $(b_1, b_2) = (p, -(p-2))$ or $(p(p-2), -(p-2)$, then equation (**??**) again implies $z_1, z_2 \in \mathbb{Z}_p$ and reduces to

$$z_2^2 \equiv -1 \pmod p$$

which has no solutions in $\mathbb{Q}_p$ since $p \equiv 3 \pmod 4$.

14. Adding the pairs from (13) to the points in $E[2]$ yields these $\mathbb{Q}_p$non-trivial pairs.

15. If $(b_1, b_2) = (p(p-2), -1)$, then equation (1) implies $z_1, z_2 \in \mathbb{Z}_p$ and reduces to

$$z_2^2 \equiv 2 \pmod{p-2}$$

which has no solutions in $\mathbb{Q}_{p-2}$ since $p - 2 \equiv 5 \pmod 8$.

16. Adding the pair from (15) to the points in $E[2]$ yields these $\mathbb{Q}_{p-2}$-non-trivial pairs.

This table reveals that the only elements of $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$ in the image of the map ϕ are those we got from $E[2]$, and Theorem 2 then implies

$$E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \mathbb{Q}(S,2) \times \mathbb{Q}(S,2) \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Since we showed before that $E_{\text{tors}} = E[2]$, we know

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times (\mathbb{Z}/2\mathbb{Z})^2,$$

hence

$$E(\mathbb{Q})/2E(\mathbb{Q}) \equiv (\mathbb{Z}/2\mathbb{Z})^{2+r}.$$

Thus, we have shown that the rank of E is $r = 0$, and we have $E \cong (\mathbb{Z}/2\mathbb{Z})^2$. $\square$

3 Proving Theorem 1(b)

Proving Theorem 1(a) was somewhat long and tedious, but it was not very difficult. To establish the bound of the rank of our curve when $p \equiv 5 \pmod 8$, we will need a more general form of 2−descent. First we restate the theorem to be proved.

Theorem 1(b). *Let p and $p-2$ be prime numbers in $\mathbb{Z}$ with $p \equiv 5$ (mod 8). Then the elliptic curve $E(\mathbb{Q})$ given by*

$$E : y^2 = x(x-p)(x-2)$$

has rank at most 1. In particular, it is either of the form

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

or

$$E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

To prove this, we use the method of 2-descent described in chapter X of Silverman [1] as Proposition 4.9, which we now state.

Theorem 3. (Descent via Two-Isogeny.) *Let $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ be elliptic curves given by equations*

$$E : y^2 = x^3 + ax^2 + bx \text{ and } E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X;$$

and let

$$\phi : E \to E' \quad \phi(x, y) = (y^2/x^2, y(b - x^2)/x^2)$$

be the isogeny of degree 2 with kernel $E[\phi] = \{\mathcal{O}, (0, 0)\}$. Let S consist of ∞ and the places dividing $2b(a^2 - 4b)$, an let $\mathbb{Q}(S, 2)$ be defined as before. There is an exact sequence

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to \mathbb{Q}(S, 2) \to WC(E/\mathbb{Q})[\phi]$$

$$\mathcal{O} \to 1$$
$$(0, 0) \to a^2 - 4b \quad d \to \{C_d/\mathbb{Q}\},$$
$$(X, Y) \to X$$

where $C_d/\mathbb{Q}$ is the homogeneous space for $E/\mathbb{Q}$ given by the equation

$$C_d : dq^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

The ϕ−Selmer group is then

$$S^{(\phi)}(E/\mathbb{Q}) \cong \{d \in \mathbb{Q}(S, 2) : C_d(\mathbb{Q}_\nu) \neq \varnothing \text{ for all } \nu \in S\}.$$

This method of $2-$descent is obviously more complicated than the first version we used. The theory behind this method is high-powered, and the interested reader is encouraged to see Silverman [1]. We will say only a few words about this theorem before using it to prove Theorem 1(b).

First, we did not previously define $WC(E/\mathbb{Q})$; this is the Weil-Ch$\hat{a}$telet group for $E/\mathbb{Q}$, which is the set of equivalence classes of homogeneous spaces for $E/\mathbb{Q}$. A homogeneous space for $E/\mathbb{Q}$ is a "twist" of the elliptic curve E, or some smooth curve on which E has a simply transitive algebraic group action. What is important about these homogeneous spaces is that they encode certain information about the elliptic curve E, and Theorem 3 says that we are able to calculate the Selmer group $S^{(\phi)}$ of our isogeny ϕ by looking at these homogeneous spaces over local fields.

What, then, is the Selmer group? This, too, should be investigated in Silverman [1]. Essentially, the Selmer group contains the homogeneous spaces which have $\mathbb{Q}_\nu$-rational points for every ν. The important thing about $S^{(\phi)}$ is that we have an exact sequence

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to S^{(\phi)}(E/\mathbb{Q}) \to \text{Ш}(E/\mathbb{Q})[\phi] \to 0.$$

The Shafarevich-Tate group Ш is essentially the group of homogeneous spaces for E which have a $\mathbb{Q}_\nu$-rational point for every place ν but no $\mathbb{Q}-$rational points; again, see Silverman [1]. Together, the Selmer and Sha groups measure the failure of the Hasse principle for these curves. Finally, computing both $S^{(\phi)}$ and $S^{(\hat{\phi})}$ and using the above exact sequence together with the exact sequence

$$0 \to \frac{E'(\mathbb{Q})[\hat{\phi}]}{\phi(E(\mathbb{Q})[2]} \to \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \to \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \to \frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} \to 0,$$

we can compute $E(\mathbb{Q})/2E(\mathbb{Q})$ as before and thus deduce the rank of E.

Before proving Theorem 1(b), we first prove two lemmas which will greatly simplify the proof of the theorem.

Lemma 1. *Given the curves*

$$E: y^2 = x^3 - (p+2)x^2 + 2px \text{ and } E': y^2 = x^3 + 2(p+2)x^2 + (p-2)^2x$$

and the isogeny

$$\phi : E \to E' \quad \phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(2p-x^2)}{x^2}\right),$$

the selmer group $S^{(\phi)}$ is

$$S^{(\phi)} = \{1, -1\}.$$

Proof of Lemma 1. We first note that Ker $\phi = \{\mathcal{O}, (0,0)\}$ and

$$E[2] = \{\mathcal{O}, (0,0), (2,0), (p,0)\} \textit{ and } E'[2] = \{\mathcal{O}, (0,0)\}.$$

Also, we have $2b(a^2-4b) = 4p(p-2)^2$, so the set $\mathbb{Q}(S,2)$ is

$$\mathbb{Q}(S,2) = \{\pm1, \pm2, \pm p, \pm(p-2), \pm 2p, \pm 2(p-2), \pm p(p-2), \pm 2p(p-2)\}.$$

For each $d \in \mathbb{Q}(S,2)$, we must check whether the associated homogeneous space

$$C_d : dw^2 = d^2 + 2(p+2)dz^2 + (p-2)^2 z^4$$

has points over each local field $\mathbb{Q}_q$ for $q = 2, p, p-2$. From Theorem 3, we have

$$\mathcal{O}, (0,0) \to 1$$

and so $d = 1 \in S^{(\phi)}$, and it remains to check whether the remaining $d \in \mathbb{Q}(S,2)$ are in the Selmer group.

1. $d = \pm p$

   We present the argument for C_p to show that $d = p$ is not in the Selmer group; the argument for C_{-p} is identical. Our homogeneous space is

   $$C_p : pw^2 = p^2 + 2(p+2)pz^2 + (p-2)z^4.$$

   Now, we have that the $p-$adic valuation of the left-hand side, $\nu_p(\text{LHS})$, is odd. Hence, the valuation of the right-hand side must also odd. But we have
   $$\nu_p(\text{RHS}) = \min\{2, 1+2k, 4k\} \text{ where } k = \nu_p(z).$$

   (We have equality in the above expression since no two of $2, 1+2k$, and 4 can ever be the same.) If $k \leq 0$, then this minimum equals $4k$, which is even. Similary, if $k > 0$, then the minimum is 2. In neither case can the valuations of the left- and right-hand sides match, so C_p has no $\mathbb{Q}_p$-rational points. Hence $\pm p \notin S^{(\phi)}$.

2. $d = \pm 2$

   We present the argument for C_2 to show that $d = 2$ is not in the Selmer group; the argument for C_{-2} is identiical. Our homogeneous space is

   $$C_2 : 2w^2 = 2^2 - 2^2(p+2)z^2 + (p-2)^2 z^4.$$

   The $2-$adic valuation of the left hand side is odd, while

   $$\nu_2(\text{RHS}) \geq \min\{2, 2+2k, 4k\} \text{ where } k = \nu_2(z).$$

   Since $\nu_2(\text{RHS})$ must be odd, we must have at least two of 2, $2+2k$, and $4k$ be equal and minimal; this is easily seen to be impossible, hence C_2 has no $\mathbb{Q}_2$-rational points. Thus $\pm 2 \notin S^{(\phi)}$.

3. $d = \pm 2p$

   Either of the two arguments above show that $\pm 2p \notin S^{(\phi)}$.

   Notice that since $S^{(\phi)}$ is a group, we have

$$\pm 2(p-2), \pm 2p(p-2), \pm p(p-2) \notin S^{(\phi)}.$$

   It remains to check whether C_d has $\mathbb{Q}_q$-rational points for $d \in \{-1, \pm(p-2)\}$ and $q \in \{2, p, p-2\}$.

4. $d = -1$

   Our homogeneous space is

$$C_{-1} : -w^2 = 1 - 2(p+2)z^2 + (p-2)^2 z^4.$$

   We show that C_{-1} has $\mathbb{Q}_q$-rational points for each $q \in \{2, p, p-2\}$, hence $-1 \in S^{(\phi)}$.

   (a) $q = 2$ We find a solution in $\mathbb{Q}_2$ as follows. Let

$$f(w,z) = 1 - 2(p+2)z^2 + (p-2)^2 z^4 + w^2.$$

   Then we have

$$\begin{aligned} f(2,1) &= 1 - 2(p+2) + (p-2)^2 + 4 \\ &= 5 - 2(7+8k) + (3+8k)^2 \\ &\equiv 5 - 14 - 16k + 9 + 16k \pmod{32} \text{ since } p \equiv 5 \pmod 8 \\ &\equiv 0 \pmod{32}. \end{aligned}$$

   So $\nu_2(f(2,1)) \geq 5$, but

$$\frac{\partial f}{\partial w} = 2w\Big|_{(w,z)=(2,1)} = 4,$$

   so $2\nu_2(\partial f/\partial w) = 4 < 5$. Hence by Hensel's lemma this lifts to a solution in $\mathbb{Q}_2$.

   (b) $q = p$

   We find a solution in $\mathbb{Q}_p$ as follows. With $f(w,z)$ as before, we have

$$f(w,z) = 1 - 4z^2 + 4z^4 + w^2 \pmod p,$$

   hence

$$f(w_0, 0) = 1 + w^2 \equiv 0 \pmod p$$

   has a solution w_0 since $p \equiv 4 \pmod 8$. Since $p \not| w_0$ and p is an odd prime, we have

$$\frac{\partial f}{\partial w} = 2w\Big|_{(w,z)=(w_0,0)} \neq 0 \pmod p,$$

   so by Hensel's lemma this lifts to a solution in $\mathbb{Q}_p$.

(c) $q = p - 2$

We find a solution in $\mathbb{Q}_{p-2}$ as follows. With $f(w,z)$ as before, we have

$$f(w,z) \equiv 1 - 2(p+2)z^2 + w^2 \pmod{(p-2)^2}$$

so

$$f(w,0) \equiv 1 + w^2 \equiv 0 \pmod{(p-2)^2}$$

has a solution w_0 since $(p-2)^2 \equiv 1 \pmod 4$. Once again, we have

$$\frac{\partial f}{\partial w} = 2w\Big|_{(w,z)=(w_0,0)} \not\equiv 0 \pmod{(p-2)}$$

so by Hensel's lemma this lifts to a solution in $\mathbb{Q}_{p-2}$.

Thus, we have $-1 \in S^{(\phi)}$. We now show that $C_{-(p-2)}$ has no $\mathbb{Q}_2-$rational points, hence $-(p-2) \notin S^{(\phi)}$. Since $S^{(\phi)}$ is a group, this will imply $(p-2) \notin S^{(\phi)}$, completing our calculation of $S^{(\phi)}$.

5. $d = -(p-2)$

Our homogeneous space is

$$C_{-(p-2)} : -(p-2)w^2 = (p-2)^2 - 2(p+2)(p-2)z^2 + (p-2)z^4.$$

We will show this space has no points over $\mathbb{Q}_2$. Let $\nu_2(w) = k, \nu_2(z) = j$. Suppose there is a solution (w,z). We have

$$\nu_2(\text{LHS}) = 2k$$

and

$$\nu_2(\text{RHS}) \geq \min\{0, 1+2j, 4j\}.$$

There are two cases to consider.

Suppose $j > 0$, which implies $k = 0$. Then $w, z \in \mathbb{Z}_2$ with w odd and z even, so

$$f(w,z) \equiv (p-2)^2 + (p-2)w^2 \equiv 1 + 3w^2 \pmod 8$$

which has no solutions. Having no solutions modulo 8 implies that there are no solutions in $\mathbb{Q}_2$.

Now suppose $j = 0$, which implies $k \geq 0$. Then $w, z \in \mathbb{Z}_2$ and z is odd. We examine $f(w,z)$ modulo different powers of 2 to gain information about w and z. Remember that $p \equiv 5 \pmod 8$. Looking modulo 2 yields

$$f(w,z) \equiv 1 + 1 + w^2 \pmod 2$$

since z is odd, so this implies w is even.

Looking modulo 2^2 and 2^3 yields no new information, so we look modulo 2^4. Note that $(p-2)^2 \equiv 9$ and $(p+2)(p-2) \equiv 5$ modulo 2^4. Then, writing $z = 1 + 2r$, $w = 2s$, and $p = 5 + 8l$, we have

$$\begin{aligned} f(w,z) &\equiv 9 - 10(1+2r)^2 + 9(1+2r)^4 + (3+8l)(2s)^2 \pmod{16} \\ &\equiv 8 + 12s^2 \pmod{16} \end{aligned}$$

and having this equal to 0 modulo 16 is equivalent to having

$$2 + 3s^2 \equiv 0 \pmod 4$$

which has no solutions. This implies that there are no solutions to $f(w,z) = 0$ in $\mathbb{Q}_2$.

Now suppose $j < 0$, which implies $k = 2j$. Changing the signs of j and k, write $w = 2^{-2j} w_0$ and $z = 2^{-j} z_0$, where w_0 and z_0 are both odd. The equation defining our homogeneous space is then

$$-(p-2)2^{-4j} w_0^2 = (p-2)^2 - 2(p+2)(p-2)2^{-2j} z_0^2 + (p-2)^2 2^{-4j} z_0^4.$$

Multiplying through by 2^{4j}, this becomes

$$-(p-2)w_0^2 = 2^{4j}(p-2)^2 - (p+2)(p-2)2^{2j+1} z_0^2 + (p-2)^2 z_0^4,$$

and looking at the resulting function modulo 8 yields

$$\begin{aligned} f(w,z) &\equiv (p-2)^2 z_0^4 + (p-2) w_0^2 \pmod 8 \\ &\equiv z_0^4 + 3w_0^2 \pmod 8. \end{aligned}$$

Since z_0, w_0 are odd, we have $f(w,z) \equiv 4 \neq 0$ modulo 8. Since there are no solutions modulo 8, there are no solutions in $\mathbb{Q}_2$.

We conclude that $-(p-2) \notin S^{(\phi)}$, and since $-1 \in S^{(\phi)}$, we have $(p-2) \notin S^{(\phi)}$. Thus, $S^{(\phi)} = \{1, -1\}$. $\square$

Lemma 2. *Given the curves*

$$E' : Y^2 = X^3 + 2(p+2)X^2 + (p-2)X \text{ and } E : y^2 = x^3 - (p-2)x^2 + 2px$$

and the isogeny

$$\hat{\phi} : E' \to E \quad \hat{\phi}(X,Y) = \left(\frac{y^2}{x^2}, y\frac{p-2-x^2}{x^2} \right)$$

the selmer group $Sel^{((\hat{\phi}))}$ *is*

$$S^{(\hat{\phi})} = \{1, 2, p, 2p\}.$$

Proof of Lemma 2.

We first note that $\mathrm{Ker}\hat{\phi} = \{\mathcal{O}, (0,0)\}$ and

$$E[2] = \{\mathcal{O}, (0,0), (2,0), (p,0)\} \text{ and } E'[2] = \{\mathcal{O}, (0,0)\}.$$

Our set $\mathbb{Q}(S,2)$ is once again

$$\mathbb{Q}(S,2) = \{\pm 1, \pm 2, \pm p, \pm(p-2), \pm 2p, \pm 2(p-2), \pm p(p-2), \pm 2p(p-2)\}.$$

For each $d \in \mathbb{Q}(S,2)$, we must check whether the associated homogeneous space

$$C_d : dw^2 = d^2 - 4(p+2)dz^2 + 2pz^4$$

has points over each local field $\mathbb{Q}_q$ for $q = 2, p, p-2$. From Theorem 3, we have

$$\mathcal{O} \to 1 \quad (0,0) \to 2p \quad (2,0) \to 2 \quad (p,0) \to p$$

and so $\{1, 2, p, 2p\} \subset S^{\hat{\phi}}$; it remains to check whether the remaining $d \in \mathbb{Q}(S,2)$ are in the Selmer group. The set of d which remain to be checked is

$$\{-1, -2, -p, \pm(p-2), \pm 2p, \pm 2(p-2), \pm p(p-2), \pm 2p(p-2)\}.$$

We proceed as in the last lemma, only this time less work is necessary. Consider $d = \pm(p-2)$; we show that C_{p-2} has no solutions over $\mathbb{Q}_{p-2}$, and the argument for $d = -(p-2)$ is identical. Our homogeneous space is

$$C_{p-2} : \pm(p-2)w^2 = (p-2)^2 \pm 4(p+2)(p-2)z^2 + 2pz^4$$

Letting $k = \nu_{p-2}(w) = k$ and $\nu_{p-2}(z) = j$, we have $\nu_2(\text{LHS}) = 1 + 2k$ and $\nu_2(\text{RHS}) \geq \min\{2, 1+2j, 4j\}$, which implies $j = k = 0$, hence $w, z \in \mathbb{Z}_{p-2}$, and in particular, $(p-2)$ does not divide w, z. Taking as our function

$$f(w,z) = (p-2)^2 \pm 4(p+2)(p-2)z^2 + 2pz^4 \mp (p-2)w^2,$$

then looking at the function modulo $p-2$ yields

$$f(w,z) \equiv 4z^4 \pmod{(p-2)}$$

which has no solutions (w,z) with $p-2 \not| z$, hence $f(w,z)$ has no solutions in $\mathbb{Q}_{\pm(p-2)}$. We conclude that $\pm(p-2) \notin S^{(\hat{\phi})}$. But by the group structure of $S^{(\hat{\phi})}$, this eliminates all of the other possible $d \in \mathbb{Q}(S,2)$. Hence we have $S^{(\hat{\phi})} = \{1, 2, p, 2p\}$. $\square$

We now prove the theorem.

Proof of Theorem 1(b).
First we show that $E_{\text{tors}} = E[2] \cong (\mathbb{Z}/2Z)^2$. Suppose $p > 5$. As in the proof of Theorem 1(a), 3 is a prime of good reduction. Since $p \equiv 5 \pmod 8$, we have $p \equiv 2 + 2k \pmod 3$ for some $0 \leq kleq2$. But if $k = 2$, then $p \equiv 0 \pmod 3$ and

is not prime (since $p > 5$). Similarly, if $k = 0$, then $p - 2 \equiv 0 \pmod 3$ and so is not prime (since $p > 5$ implies $p - 2 > 3$). Then one easily checks that

$$E(\mathbb{F}_3) = \{\mathcal{O}, (0,0), (1,0), (2,0)\},$$

and since $E_{tors} \hookrightarrow E(\mathbb{F}_3)$ and $E[2] \subset E_{\text{tors}}$, we have

$$E_{\text{tors}} = E[2] \cong (\mathbb{Z}/2Z)^2.$$

If $p = 5$, one easily checks that

$$E(\mathbb{F}_7) = \{\mathcal{O}, (0,0), (1,2), (1,5), (2,0), (3,1), (3,6), (5,0)\} \cong (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

and a similar argument gives the desired result.

Now we compute the rank. To apply Theorem 3, we need to compute precisely the Selmer groups from Lemmas 1 and 2. Having computed both Selmer groups, we may now use the exact sequences mentioned earlier to compute the rank of E. Recall that we have the following exact sequences:

$$0 \to \frac{E'}{\phi(E)} \to S^{\phi}(E) \to \text{Ш}(E)[\phi] \to 0 \tag{3}$$

$$0 \to \frac{E}{\hat{\phi}(E)} \to S^{\hat{\phi}}(E) \to \text{Ш}(E')[\hat{\phi}] \to 0 \tag{4}$$

$$0 \to \frac{E'[\hat{\phi}]}{\phi(E[2])} \to \frac{E'}{\phi(E)} \to \frac{E}{2E} \to \frac{E}{\hat{\phi}(E')} \to 0 \tag{5}$$

Now, we have computed

$$S^{(\phi)} \cong \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad S^{(\hat{\phi})} \cong (\mathbb{Z}/2\mathbb{Z})^2,$$

and we actually showed that every point in $S^{(\hat{\phi})}$ came from a point on our curve, hence $\text{Ш}(E')[\hat{\phi}] = 0$. Sequence (4) then implies

$$E/\hat{\phi}(E) \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

It is also easy to check that $\phi(E[2]) = E'[\hat{\phi}]$, hence $E'[\hat{\phi}]/\phi(E[2]) = 0$. Thus, sequence (5) becomes

$$0 \to \frac{E'}{\phi(E)} \to \frac{E}{2E} \to (\mathbb{Z}/2\mathbb{Z})^2 \to 0. \tag{6}$$

We do not know if $\text{Ш}(E)[\phi] = 0$; thus, from sequence (3) we have

$$0 \to \frac{E'}{\phi(E)} \to \mathbb{Z}/2\mathbb{Z} \to \text{Ш}(E)[\phi] \to 0,$$

so we have either $\frac{E'}{\phi(E)} \cong \mathbb{Z}/2\mathbb{Z}$ or 0; comparing the orders of the groups in (6) shows that $\text{rank}(E) = 1$ in the first case and 0 in the second, proving the theorem. $\square$

4 Acknowledgements

The author would like to thank Dr. Thomas Hagedorn for all of his help and guidance with this paper, and Jason Beers for making the conjectures that feature as this paper's theorems. This paper was written in partial fulfilment of graduation requirements at The College of New Jersey.

5 References

[1] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag. New York, NY, 1986.